Information and Privacy
Commissioner/Ontario

Commissaire à l'information
et à la protection de la vie privée/Ontario

Privacy Assessment:

The University Health Network's Response to Recent Breaches of Patient Privacy

July 30, 2002

80 Bloor Street West
Suite 1700
Toronto, Ontario
M5S 2V1

80, rue Bloor ouest
Bureau 1700
Toronto (Ontario)
M5S 2V1

416-326-3333
1-800-387-0073
Fax/Téléc: 416-325-9195
TTY: 416-325-7539
Web site: www.ipc.on.ca

Information and Privacy
Commissioner/Ontario

80 Bloor Street West
Suite 1700
Toronto, Ontario
M5S 2V1

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Web site: www.ipc.on.ca

This publication is also available on the IPC Web site.

Table of Contents

Introduction 1
- University Health Network 1
- UHN's Clinical Information System 1
- UHN's Confidentiality Policy 2
- UHN's Auditing Program 3
- UHN Discovers Apparent Breaches of Patient Privacy 3

Key Issue Arising in this Assessment 5

Results of the Assessment 6
- Inquiries into Apparent Privacy Breaches 6
- Reviewing Corporate Policies and Practices 8
- Privacy Training 9

Other Matters 12
- Confidentiality Agreement for Accessing Audit Report 12

Conclusion 13

Summary of Recommendations 14

Appendix A – Audit Report Confidentiality Agreement 15

Introduction

University Health Network

The University Health Network (UHN) is a 1,000-bed healthcare organization composed of three hospitals: Toronto General Hospital, Toronto Western Hospital and Princess Margaret Hospital. Collectively, these hospitals employ more than 10,000 people, including 520 full-time physicians. Over the course of a year, UHN provides healthcare for approximately 39,000 inpatients and 800,000 outpatients.

In December 2001, UHN became the first hospital system in Ontario to appoint a Corporate Privacy Officer (CPO) to oversee and manage health privacy issues. The CPO is a member of UHN's corporate management team and reports to the Chief Information Officer. UHN also has an Information Protection Services team responsible for protecting the privacy, confidentiality and security of all personal information under the custody or control of UHN in accordance with existing legislation, public expectations of privacy, and internationally accepted fair information practices.[1]

UHN supports the implementation of comprehensive health privacy legislation in Ontario. In February 2002, the Ontario government released a draft privacy bill, the *Privacy of Personal Information Act, 2002*, for public comment. The draft bill, which is based on fair information practices, would apply to the provincially-regulated private sector, the health sector (including hospitals), and other organizations such as universities and non-profit groups. The UHN made a submission to the government in March 2002 that supports the thrust of the draft legislation.

UHN's Clinical Information System

Since the mid-1990s, UHN has been moving toward replacing traditional paper charts with electronic patient records. Currently, it uses a clinical information system called Patient 1 Vista/Ulticare, which is supplied by Per-Se Technologies Inc., a company based in Atlanta, Georgia.

Patient 1 Vista/Ulticare enables UHN physicians, nurses and other staff to perform both administrative and medical functions electronically, including creating and amending patient records, entering notes about a patient's symptoms, reviewing another physician's or nurse's notes about a patient, ordering tests and treatment, checking laboratory results and admitting, discharging or transferring patients to other units within UHN. The clinical information system provides any authorized caregiver within UHN, depending on their access privileges, with the ability to access a patient's medical records on a desktop or laptop computer.

[1] The 10 fair information practices are codified in the Canadian Standards Association's *Model Code for the Protection of Personal Information*. They outline responsible information-handling practices designed to protect privacy and form the basis for virtually all privacy legislation in Canada.

More than 5,000 UHN employees have some access to the clinical information system. In order to gain access to the system, a new UHN staff member or medical resident must fill out an access request form, which must be approved by either the staff member's manager or the Vice President of Education (for medical residents). Once the access request form is approved, a new staff member or medical resident must then attend a training session on the clinical information system, which includes a discussion on privacy, confidentiality and security. After successfully completing this session, the staff member or medical resident is issued a unique user ID and password for accessing the system.

According to UHN, although paper records are still used within its hospitals, the clinical information system has greatly improved the quality of care provided to patients. For example, if a patient is receiving chemotherapy for cancer on a weekly basis at Princess Margaret Hospital but shows up one day in the emergency room at Toronto Western Hospital, the physician on duty can access that patient's records through the clinical information system. The system provides the physician with the ability to instantaneously review the patient's medical history and use that information to make an informed diagnosis and treatment decision.

UHN's Confidentiality Policy

The privacy rights of UHN patients are currently governed by a broad policy on "Confidentiality of Information and Data Security" that was implemented in 1995. Confidential information is defined as including patient information, financial information, human resources information and human rights information. The policy notes that a patient's right to privacy is based on the principle that "patients have control over what, and to whom, information about themselves is disclosed, subject to exceptions outlined in law."

Under the policy, UHN staff and other individuals who work at UHN (e.g., medical residents) are permitted to access the personal information of patients. However, this access is strictly limited to information that an individual requires for the performance of his or her hospital duties. In other words, an individual may only access the personal health information of patients for the purpose of performing his or her job duties.

UHN staff and other individuals who work at UHN are prohibited from disclosing personal health information except with the consent of the patient, for the performance of their hospital job functions, or for other limited and specific purposes set out in the policy.

The policy makes it clear that if a breach of confidentiality is found to have occurred, the result will be immediate disciplinary action, up to and including termination and loss of all hospital privileges.

All new employees and medical residents are required to sign a confidentiality agreement and to attend a general orientation session where the confidentiality agreement and policy are discussed in greater detail.

UHN's Auditing Program

With paper records, it can be difficult to monitor whether a patient's records are only being accessed for legitimate purposes. However, one significant privacy benefit of a clinical information system is that it can be designed to allow an institution to audit all access to patient records. Patient 1 Vista/ Ulticare creates an audit trail by recording the name, job title, department and date of access of UHN staff and other users, each time that they access an electronic patient record.

The confidentiality policy makes it clear that UHN conducts regular audits on patient records stored in the clinical information system. Audits are conducted monthly on the records of randomly chosen patients. In addition, UHN conducts mandatory audits on the records of well-known individuals who are patients at the three hospitals.

Both staff and medical residents receive a copy of the confidentiality policy before they commence work at UHN. The fact that accesses to patient records are audited is mentioned at the general orientation sessions for new UHN staff and medical residents and also at the clinical information system training sessions. Moreover, a warning pops up on a user's computer before he or she accesses an electronic patient record, stating that the access to the chart will be recorded. The user is then asked whether he or she wishes to continue and is given a choice of "yes" or "no."

UHN Discovers Apparent Breaches of Patient Privacy

In May 2002, two well-known individuals checked into the UHN hospital system for treatment. For the purposes of this report, these patients will be referred to as "Patient A" and "Patient B."

Patient A was an inpatient at one of the UHN hospitals for four days in May 2002. Patient B was cared for by UHN for five days in May 2002. In accordance with its confidentiality policy, UHN ran audits on the accesses by staff and other users of the clinical information system to the records of these two well-known individuals. From May 13-25, 2002, audits were done twice a day on accesses to the records of Patient A. UHN started to run audits on the records of Patient B commencing on May 25, 2002 and is continuing to run these audits on a daily basis. A privacy technical specialist from UHN's Information Protection Services team conducted the audits under the direction of the CPO.

The CPO then reviewed the audit reports and found that most of the accesses to the medical records of the two well-known patients were for job-related purposes. However, they also found that a small number of UHN staff and medical residents had accessed the records of the two well-known patients, even though they did not appear to be involved, directly or indirectly, in the care provided to these patients. All of these unusual accesses occurred within 72 hours of both patients being admitted to the hospitals at UHN.

On May 24, 2002, a reporter from *The Globe and Mail* contacted UHN and requested an interview with UHN's President and CEO, Tom Closson. During the interview, the reporter informed Mr. Closson that she was aware of the apparent breaches of patient privacy that had occurred at UHN and asked him what he was doing to address the problem.

On May 27, 2002, UHN's CPO contacted the IPC to inform us of the apparent breaches of patient privacy. Later in the day, the CPO met with the IPC's Director of Policy and Compliance and me. Currently, the IPC does not have oversight or jurisdiction over the health sector, including hospitals. However, I suggested that my office conduct an independent assessment of UHN's response to the privacy breaches that had allegedly occurred. The CPO passed on my suggestion to Mr. Closson, who accepted.

On May 28, 2002, an article appeared in *The Globe and Mail* that reported that UHN was calling in the IPC after an internal audit revealed that several employees might have inappropriately looked at patients' medical records. In the article, Mr. Closson emphasized that he had called in the IPC, not as a result of the news stories, but because of the findings of the internal audit.

On May 30, 2002, the IPC's Director of Policy and Compliance and I met with Mr. Closson and his CPO to discuss the parameters for the assessment. Under the terms of reference that were subsequently agreed upon between UHN and the IPC, my office had access to UHN policies and relevant staff, but we did not have access to identifiable patient information or the individuals who had inappropriately accessed patient records.

Over the past two months, my staff has held four meetings and numerous phone interviews with UHN's CPO and her staff to gather information about UHN's response to the results of the audits that were run on the electronic records of the two well-known patients. In addition, I was provided with the opportunity to review an audit report of accesses to my records during the periods I had been a patient at UHN. During the course of our assessment, my staff received full co-operation from UHN's senior management and CPO.

Key Issue Arising in this Assessment

In accordance with the UHN/IPC terms of reference, this report will be addressing the following key issue:

- Is UHN making reasonable efforts to ensure that the privacy breaches that occurred regarding inappropriate access to electronic patient records do not happen again?

Personal health information is one of the most sensitive forms of personal information. A patient record might contain information about abortions, sexually transmitted diseases, heart conditions, depression, drug abuse or other matters that individuals may not want shared with anyone else except for their caregivers. As a result, if a healthcare institution discovers that its staff or other individuals have inappropriately accessed patient records, it should take immediate steps to address the breaches of privacy and make "reasonable efforts" to ensure that such breaches do not recur.

What would constitute "reasonable efforts" by UHN? In my view, "reasonable efforts" can be defined as what a privacy-conscious and prudent healthcare institution would do in similar circumstances. This would include:

- Conducting an immediate investigation of the privacy breaches that allegedly occurred and, if necessary, taking appropriate disciplinary action against the individuals who are found to have violated any privacy laws or policies.
- Reviewing the institution's corporate policies and practices, including those relating to privacy, to determine if they can be improved.
- Putting in place intensive privacy training for both new and existing staff.

Results of the Assessment

During the course of our assessment, my staff found that UHN had taken a number of steps to address the breaches of patient privacy that were detected in the audit reports and to ensure that similar breaches did not recur:

Inquiries into Apparent Privacy Breaches

After the CPO reviewed and signed the audit results, inquiries were commenced into each of the unexplained accesses to determine if the privacy rights of the two well-known patients had been breached.

The CPO contacted the supervisors of each of the individuals subject to an inquiry and asked them if they could explain why their staff member or medical resident had used the clinical information system to access the records of the well-known patients. If the individual's supervisor was able to provide a reasonable explanation for the suspicious access, he or she was asked to put the explanation in writing. If the supervisor could not explain why his or her staff member or medical resident had accessed the records of a well-known patient, a fact-finding meeting was scheduled with that individual.

UHN held fact-finding meetings on May 22, 23, 24, 27 and 29. The meetings included the following persons, depending on whether the individual subject to an inquiry was a UHN staff member or a medical resident: the individual's supervisor, a representative from the human resources department, a union representative (if the staff member was a union member), the Vice President of Education (if the individual was a medical resident), and the CPO. The Vice President of Education was not able to attend all of the fact-finding meetings. In such cases, a medical resident's direct supervisor and/or his or her department head attended the meeting.

After the fact-finding meetings, six individuals subject to an inquiry were sent home with pay and had their access to the clinical information system turned off. They were also informed that UHN would contact them once a final decision had been rendered on their particular case.

During the course of the inquiries, UHN's President and CEO telephoned Patients A and B to inform them that their electronic patient records may have been inappropriately accessed. He also apologized for any privacy breaches that may have occurred.

On May 30, 2002, UHN senior management held a decision-making meeting, which included the President and CEO, the Chief Information Officer and Vice President, the CPO, the Vice President of Human Resources, and the Vice President of Medical Education. After considering all the evidence, the President and CEO made a final decision in each case, in conjunction with either the Vice President of Human Resources (for UHN staff) or the Vice President of Education (for medical residents).

Ultimately, six individuals were found to have inappropriately accessed patient records: three UHN staff members and three medical residents. The Vice President of Human Resources (for UHN staff) and the Vice President of Education (for medical residents) sent letters to the violators on May 30 and 31. The discipline that was issued ranged from a reprimand to a 14-day suspension without pay. The decision letters have been added to each individual's employment file. In addition, the supervisors for each of the disciplined individuals have spoken to them personally about the importance of respecting patient privacy.

The UHN staff who were disciplined are also being required to attend mandatory privacy training sessions on a bi-weekly or monthly basis. The CPO's office is providing the content for these sessions, which will focus on a variety of privacy topics, including the application of fair information practices in a healthcare environment. The medical residents who were disciplined are being required to attend four to six privacy sessions during the summer months. The CPO is also providing privacy content for these sessions, which are being run by the Joint Centre for Bioethics at the University of Toronto.

I believe that UHN should be praised for acting quickly after discovering the apparent breaches of patient privacy in their audit reports. The swift initiation and conclusion of the inquiries demonstrates to both staff and the public that UHN is serious about protecting patient privacy. The disciplinary measures will also serve to deter the individuals concerned and their peers from committing similar acts in the future. More importantly, however, the mandatory training sessions will help the individuals who inappropriately accessed electronic patient records to understand in greater depth why it is important to respect the privacy rights of patients.

I also commend UHN for quickly notifying its other staff and medical residents about the breaches of patient privacy, and for reminding them about the importance of protecting the personal health information of their patients. On May 27, 2002, the President and CEO sent out an e-mail message to all staff that informed them that, "UHN recently performed electronic audits of our clinical information systems and some incidents were identified where staff may have inappropriately accessed the electronic records of individual patients."

The e-mail, which was also published on the front page of the June 3, 2002 issue of the institution's newsletter, *UHN News*, refers staff to UHN's confidentiality policy and points out that disciplinary actions for breaching patient privacy could include verbal or written warnings, suspensions or dismissal. It also provides staff with some practical tips for protecting patient privacy, including:

- Employees accessing patient records through Vista/Ulticare should only access information on patients for whom they are delivering care or are directly involved with for legitimate hospital business.
- Do not share your computer password and user ID. You will be responsible for any inappropriate access to information obtained using your ID.

- Do not discuss confidential information where others may overhear you, such as in elevators, food courts, hallways or on the shuttle bus.
- Shred all print-outs or paper waste containing confidential information.
- Log out of your computer when you are finished.

I believe that the President and CEO's e-mail/newsletter article is a strong indicator that UHN is making reasonable efforts to ensure that the privacy breaches that occurred do not happen again.

Reviewing Corporate Policies and Practices

UHN has also taken other steps to ensure that the inappropriate accesses to electronic patient records do not happen again. After UHN discovered the breaches of patient privacy, it accelerated a review of its corporate policies and practices that had been initiated by its CPO shortly after she was hired.

First, it invited privacy expert David Flaherty, the former Information and Privacy Commissioner of British Columbia, to conduct an independent review of its overall privacy practices. Professor Flaherty, who is now a privacy consultant, visited all three UHN hospitals in late May and will be submitting a report to UHN that covers a variety of privacy issues, including the security of UHN's medical records and privacy training for volunteers. I believe that seeking the advice of an independent third party is another indicator that UHN is making reasonable efforts to ensure that the privacy breaches that occurred do not happen again.

Second, UHN has also conducted a review of the specific access privileges that both UHN staff and medical residents have to patient records on the clinical information system. UHN informed us that access privileges for various users are on a "need-to-know" basis and vary depending on an individual's specific job duties. For example:

- Physicians, medical residents and most nurses have full access to all patient records at UHN.
- Some health professionals, such as occupational therapists and physiotherapists, have access only to the records of patients who are being treated in their particular clinic.
- Nutritionists and dieticians have access only to demographic and other necessary information about a patient (e.g., name, address and phone number, information about a patient's allergies).
- Switchboard operators only have "patient inquiry" access to patient records, which means that they can only access information about the patient's location within UHN and his or her status. If a patient does not want to receive a phone call from a particular individual, this information would also appear on the switchboard operator's computer screen.

UHN concluded that the existing access privileges granted to staff and medical residents are appropriate. The full access to patient records available to physicians, medical residents and most nurses is deemed necessary because UHN provides multidisciplinary care, and patients may move from unit to unit within the UHN hospitals. In addition, the conduct of periodic audits on accesses to electronic patient records is meant to deter staff from inappropriately accessing such records. While I believe that UHN should periodically review the access privileges that it grants to both UHN staff and medical residents, I do not disagree with UHN's position that the access privileges that currently exist appear to be appropriate.

Third, UHN was in the process of replacing its existing confidentiality policy with a privacy policy when the inappropriate access to patient records occurred. The draft privacy policy focuses on the application of fair information practices in a healthcare context. UHN is aiming to approve and implement the policy in the summer or fall of 2002. In addition, the CPO will be monitoring the progress of the Ontario government's proposed private-sector and health privacy bill and will amend the UHN privacy policy accordingly if the bill is enacted into law.

My office has received a copy of the draft privacy policy and will be providing UHN with our comments shortly after this report is published. Upon receiving our comments, UHN should approve its draft privacy policy as soon as possible.

Recommendation #1

UHN should finalize and approve its draft privacy policy no later than October 1, 2002.

Privacy Training

In a further effort to ensure that the inappropriate accesses to patient records do not happen again, UHN is reforming its corporate training for both staff and medical residents.

UHN Staff

UHN's human resources department conducts corporate orientation sessions for new staff. Before the privacy breaches occurred, the discussion on confidentiality during the orientation lasted for 10 to 20 minutes depending on the number of questions posed by staff. The new section on confidentiality will focus more narrowly on privacy issues and last for up to 30 minutes. It will include a discussion of the fair information practices found in the Canadian Standards Association's *Model Code for the Protection of Personal Information*, and an explanation of the differences between privacy, confidentiality and security. Staff will also be informed about the UHN's draft privacy policy, which will be discussed in greater detail at the orientation sessions once it is approved.

Moreover, the CPO will be working with UHN's human resources department to offer ongoing privacy training for existing staff. During the past two months, the CPO has already run some *ad hoc* privacy sessions with various groups of employees (e.g., occupational therapists) but a more strategic training program will be rolled out in the fall once the draft privacy policy is approved.

UHN is also examining the possibility of integrating a discussion about privacy into the annual performance review meeting that each manager holds with each of his or her employees. This may include discussing the relevance of fair information practices and UHN's privacy policy (after it is approved) to an employee's specific job.

Finally, UHN is considering the feasibility of producing a new staff training video that focuses on privacy, and purchasing a Web-based learning module on privacy that could be used by those staff and medical residents who have access to the UHN computer network.

Medical Residents

In general, medical residents start work at UHN in July and January of each year. The Medical Education Office orients new residents. This orientation is similar to the orientation for new UHN staff but residents are also given a copy of the CSA *Model Code* and directed to Web sites where they can read articles on privacy. After the orientation session, residents meet with the Medical Education Co-ordinator, who discusses fair information practices with them in greater detail. At the end of this meeting, all residents must sign a form that acknowledges that they have read the fair information practices that were provided to them in written form.

The majority of medical residents at UHN have completed or are completing a four-year undergraduate degree in medicine (M.D.) at the University of Toronto's Faculty of Medicine. According to the Faculty's Web site, ethics instruction for medical students at the University of Toronto stretches over the length of the undergraduate program, including 18 hours in both the first and second years of medical school, 8 hours in the third year and 15 hours in the fourth year. The core teaching in ethics is reinforced by the topic of professionalism, which includes issues such as confidentiality and privacy.[2]

During our second meeting with UHN's CPO, she indicated that her office plans to work with the University of Toronto's Faculty of Medicine to enhance the teaching of ethics to students who are destined for medical residencies at UHN. At that time, I suggested that UHN propose to the Faculty of Medicine that it bring in a privacy specialist – such as myself, my staff or other experts – to speak to medical students. UHN may also wish to consider approaching all of the Ontario medical schools from which it draws students and suggest that more privacy training be integrated into the undergraduate curriculum.

[2] www.library.utoronto.ca/medicine/curric/me.htm

Recommendation #2

UHN should propose to the University of Toronto's Faculty of Medicine and other Ontario medical schools that the undergraduate curriculum for medical students includes at least eight hours of lectures and workshops run by privacy specialists. These lectures and workshops should focus specifically on the importance of protecting the privacy of personal health information, and include a discussion of relevant privacy legislation and the practical application of fair information practices in a healthcare environment.

Other Matters

Confidentiality Agreement for Accessing Audit Report

Any person who is or has been a patient at a UHN hospital is permitted to see an audit report of accesses by staff and other users of the clinical information system to his or her electronic patient records. During the course of this assessment, I was provided with the opportunity to review an audit report of accesses to my records during the periods I had been a patient at UHN.

In general, I was very pleased with the substance of the audit report, which is clear and easy to understand. The report shows the name, job title, department and date of access of UHN staff and other users, each time they accessed my electronic patient records. I did not see any accesses that seemed to be inappropriate or questionable.

However, I do have a concern about the confidentiality agreement that patients are required to sign, which is attached as Appendix A of this report. In order to access an audit report, patients or their authorized representatives must sign and date this agreement. This in itself is not a problem with the exception of the following. At the bottom of the agreement, there is a paragraph that states, "I understand that my audit report contains confidential information on UHN physicians and staff. I agree to review this information for audit purposes only. I also agree not to disclose this information, except as it relates to my health condition or treatment."

I stroked out this paragraph before signing the agreement to signify that I did not consent to these conditions. In my view, the information about physicians and other UHN staff on the audit report is professional information, relating to professional services performed, not personal information. For example, the name, job title and department of a particular UHN physician or staff member in a publicly-funded hospital is information about that individual in his or her employment capacity, not their personal capacity, and should not be protected from disclosure.

Accordingly, patients who wish to review an audit report of accesses to their records should not be required to acknowledge that such information is "confidential," and should not be prohibited from disclosing this information.

Recommendation #3

UHN should delete the last paragraph in the confidentiality agreement that patients are required to sign before they are permitted to view an audit report of accesses by UHN staff and other users of the clinical information system to their health records.

Conclusion

In my view, UHN is making considerable efforts to ensure that the privacy breaches that occurred regarding inappropriate access to electronic patient records do not happen again. Specifically, UHN has taken the following steps:

- After discovering the apparent breaches of patient privacy, it conducted a series of swift inquiries and took disciplinary action against the individuals who were found to have inappropriately accessed electronic patient records.
- The President and CEO quickly sent out an e-mail that notified UHN staff and medical residents that electronic patient records may have been inappropriately accessed and reminded them about the importance of protecting the personal health information of patients. The e-mail was also published on the front page of UHN's staff newsletter.
- UHN invited privacy expert David Flaherty, the former Information and Privacy Commissioner of British Columbia, to conduct an independent review of its overall privacy practices.
- It conducted a review of the specific access privileges that both UHN staff and medical residents have to patient records on the clinical information system.
- It accelerated its plan to replace its existing confidentiality policy with a privacy policy that focuses specifically on the application of fair information practices in a healthcare environment.
- The orientation sessions for new staff and medical residents are being enhanced to include a greater focus on privacy issues.
- The CPO will be working with UHN's human resources department to offer ongoing privacy training for existing staff.
- UHN is examining the possibility of integrating a discussion about privacy into the annual performance review meeting that each manager holds with each of his or her employees. This may include discussing the relevance of fair information practices and UHN's privacy policy (after it is approved) to an employee's specific job.
- The CPO will be working with the University of Toronto's Faculty of Medicine in an effort to enhance the privacy training provided to medical students.

In my view, all of these measures constitute reasonable efforts and meet the standard of what a privacy-conscious and prudent healthcare institution would do in similar circumstances. In short, I am satisfied with the efforts that UHN is making to ensure that the privacy breaches that occurred do not happen again.

Summary of Recommendations

Although I have concluded that UHN is making reasonable efforts to ensure that the privacy breaches that occurred regarding inappropriate access to electronic patient records do not happen again, I would make the following recommendations:

1. UHN should finalize and approve its draft privacy policy no later than October 1, 2002.
2. UHN should propose to the University of Toronto's Faculty of Medicine and other Ontario medical schools that the undergraduate curriculum for medical students includes at least eight hours of lectures and workshops run by privacy specialists. These lectures and workshops should focus specifically on the importance of protecting the privacy of personal health information, and include a discussion of relevant privacy legislation and the practical application of fair information practices in a healthcare environment.
3. UHN should delete the last paragraph in the confidentiality agreement that patients are required to sign before they are permitted to view an audit report of accesses by UHN staff and other users of the clinical information system to their health records.

Ann Cavoukian, Ph.D.
Commissioner

July 30, 2002
Date

Appendix A – Audit Report Confidentiality Agreement

University Health Network

Toronto General Hospital Toronto Western Hospital Princess Margaret Hospital

The University Health Network is pleased to provide you with information on access to your personal health information.

The following audit report has been provided for you at your request, as a patient or authorized patient representative.

This audit report lists the names of the users on our clinical information system who accessed your personal health information while you were a patient at the University Health Network during specific visits.

If you have questions about the information contained on the audit report, please direct them to the clinical information specialist assisting you today.

_____

Patient Signature

I understand that my audit report contains confidential information on UHN physicians and staff. I agree to review this information for audit purposes only. I also agree not to disclose this information, except as it relates to my health condition or treatment.

_____

Date